CLAIMS:

1. A method for generating a common secret data item between a first user facility i and a second user facility j through by each such user facility executing mutually symmetric operations on respective complementary data items that are based on respectively unique quantities and that are at least in part secret, and wherein an outcome of said operations is used in both said user facilities as said common secret data item,

said method being characterized in being based on defining said complementary data belonging to a GAP Diffie-Hellmann Problem that is defined in an Abelian Variety.

2. A method as claimed in Claim 1, wherein said Abelian Variety has a dimension ***one*** through being an elliptic curve.

3. A method as claimed in Claim 1, comprising applying a pairing F featuring a bilinearity property, a non-degeneration property, and a computability property to two linearly independent points P and D(P) on said Abelian Variety.

4. A method as claimed in Claim 1, wherein said operations for user facility i are based on one-way functions **f, g** according to $S_i = f_T (r_i)$ and $P_i = g (r_i)$, wherein parameter **T** is a master secret acquired from a trusted master facility, outcome **S** is being maintained secret, and common secret data are calculated according to

$$K_{ij} = F (S_i , P_j) = F (S_j , P_i) = K_{ji}.$$

5. A method as claimed in Claim 4, wherein said operations base on data S_i and P_i

$S_i : s_{i1} = T_{11} + r_i T_{12}$; (5') $\quad s_{i2} = T_{21} + r_i T_{22}$; (6')

$P_i : p_{i1} = r_i P$; (7') $\quad p_{i2} = r_i^2 P$; (8').

6. A method as claimed in Claim 1, wherein user facility 1 sends data $r_1 D (P) , r_1^2 D (P)$ to user facility 2, user facility 2 sends data

$r_2 D(P), r_2^2 D(P)$ to user facility 1, followed by user facility 1 checking whether the triple
$r_2 D(P), r_2 D(P), r_2^2 D(P)$ is a Diffie-Hellmann triple, and user facility 2 whether the triple $r_1 D(P), r_1 D(P), r_1^2 D(P)$ is a Diffie-Hellmann triple, and in the positive case calculating the common secret by user facility 1 according to
$\Pi_{k=1}^2 e((t_{k1} + r_1 t_{k2}) P, v(r_2)_k D(P)) = e(P, D(P))^{\langle v(r_1), Tv(r_2)\rangle}$
wherein $t_{12} = t_{21}$ and $v(r_2)_k$ stands for the k-th component of the vector $v(r_2)$.

7. A method as claimed in Claim 1, and furthermore comprising a revocation scheme on top of its standard scheme for excluding one or more selected user facilities through assigning to every user facility its own unique parameters.

8. A method as claimed in Claim 1, wherein the generating of such shared secret is used as an initial step in an identification or authentication procedure.

9. A method as claimed in Claim 1, wherein the Weil Pairing is evaluated at an instant in time that lies substantially before executing the protocol proper.

10. A method as claimed in Claim 1, and comprising an updating of secret information against divulgation of an earlier secret information.

11. A method as claimed in Claim 1, and being executed through using only a single integrated cryptography level.

12. A method as claimed in Claim 1, where a randomization scheme is applied to the common secret.

13. A method as claimed in Claim 12, where the randomization scheme is based on a challenge-response mechanism.

14. A system comprising a first user facility and a second user facility, and being arranged to communicate according to the method as claimed in Claim 1.

15. A device being arranged to operate as the first and/or second user facility in a system as claimed in Claim 14.

16. A computer program product comprising instructions for controlling one or more data processing oriented hardware entities to implement a method as claimed in Claim 1.